UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/565,567	01/23/2006	Jorge Abellan Sevilla	09669/081001	2117

22511 7590 11/17/2009

OSHA LIANG L.L.P.
TWO HOUSTON CENTER
909 FANNIN, SUITE 3500
HOUSTON, TX 77010

EXAMINER	
KANAAN, SIMON P	

ART UNIT	PAPER NUMBER
2432	

NOTIFICATION DATE	DELIVERY MODE
11/17/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docketing@oshaliang.com
buta@oshaliang.com

Office Action Summary	Application No.	Applicant(s)	
	10/565,567	SEVILLA, JORGE ABELLAN	
	Examiner	Art Unit	
	SIMON KANAAN	2432	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 November 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-9 and 11-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *17-21* is/are allowed.

6)☒ Claim(s) *1-9, 11-12 and 14-16* is/are rejected.

7)☒ Claim(s) *13* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on **11/5/2009** has been entered.

2. Applicant's arguments/ amendments with respect to pending claims **1-9 and 11-21** filed **11/05/2009** have been fully considered and are persuasive. However, upon further search and consideration a new ground of rejection is presented below.

Allowable Subject Matter

Claims 17-21 are allowed.

Claim 13 is objected to as allowable but dependent on a rejected base claim.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1,2,6,9 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Andreaux et al. (WO 02/47356 A2) in view of Ginter et al. (US PG Publication # 2002/0048369 A1) and further in view of Kaneko (US Patant # 6,832,731 b2)

As per claims 1 and 9, Andreaux discloses: Method and device for monitoring the usage of a service by a communication device coupled to a smart card, said service being transmitted from a resource able to communicate with said communication device by way of a network, - Andreaux, page 1, lines 7 and 8, the digital data is transferred in a digital network

said service comprising a plurality of encrypted data flow, the use of said service comprising successive decryption steps of data flow by a respective first key, said first key being encrypted in the data flow – Andreaux, page 8, lines 12 through 20, the information is decrypted multiple times

and decrypted in the smart card by way of a second key stored in said smart card or derived inside said smart card, - Andreaux, page 5, lines 33 through 36, a second key is used for encryption and decryption, and page 8, lines 12 through 20, the smart card stores cryptographic keys)

characterized in that said method comprises the following steps:

but does not specifically disclose the use of a smartcard in the first embodiment of the invention.

However, Andreaux discloses a smart card in the second embodiment. –Andreaux. page 9, lines 17 through 21, smart card used

It would have been obvious for one skilled in the art at the time of the invention to store the data in memory as stated in the first embodiment of Andreaux storing data on a smart card as stated in the second embodiment of Andreaux because a smart card is a well known form for storing data.

But does not explicitly disclose a. A counting step, in which a memory location stores a count of occurrences of decryption steps of said first key attached to a same service;

However, Kaneko discloses a. A counting step, in which a memory location stores a count of occurrences of decryption steps of said first key attached to a same service; -Kaneko, figure 8, counter decremented each time data is decrypted.

It would have been obvious for one skilled in the art to modify the counter determining device usage in Andreaux with the counter determining the number of times data is decrypted in Kaneko since determining the number of times data is decrypted allows limiting the number of reproduction. – Kaneko, column 2, line 66 through column 3, line 21.

But does not disclose a using step, in which said counter is used to determine a service fee for use of said service

However, Ginter discloses a using step, in which said counter is used to determine a service fee for use of said service –Ginter, [2376] and [1070]

It would have been obvious for one skilled in the art to modify the counter determining device usage in Andreaux with the counter determining device usage which determines tampering in Ginter since determining tampering prevents misuse of product. – Ginter, [1070].

As per claim 2, Andreaux in view of Kaneko and further in view of Ginter discloses the method according to claim 1, characterized in that the smart card stores a predetermined fixed number, and in that it comprises a comparison step in which the incrementing counter is compared to the predetermined fixed number for checking if the counter has reached or not the value of the fixed number; if yes, adequate action can be performed.- Andreaux, page. 8, lines

12-20, counter is decremented, which is incrementing by -1, and compared to zero which is the predetermined fixed number. Action is performed until the counter equals zero

As per claim 6, Andreaux in view of Kaneko and further in view of Ginter discloses the method according to claim 2, characterized in that the action is the completion of decryption steps. –Andreaux, the data is encrypted and is transmitted a certain number of times with the key if the key is not equal to zero. This is part of the decryption steps.

As per claim 14, Andreaux in view of Kaneko and further in view of Ginter discloses the method according to claim 1, wherein the method further comprises upon reception of a management container: performing a retrieval of the counter; and sending management data to the resource through a protocol based in a point-to-point mechanism. –Andreaux, page 1, line 8, communication through a network which is a point-to-point mechanism

As per claim 15, Andreaux in view of Kaneko and further in view of Ginter discloses the method according to claim 1, wherein the method further comprises: associating at least two counters to a particular service; and resetting one of the at least two counters, wherein the other counter is not reset at the same time. –Ginter, column 167, lines 39-50, counters are reset, counters when reset are not reset at exactly the same time as the processor can handle only one process at a time.

As per claim 16, Andreaux in view of Kaneko and further in view of Ginter discloses the method according to claim 1, wherein the resource communicates with said communication device over a network. –Andreaux, page 1, line 8.

5. Claims 3, 5, 7 and 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Andreaux et al. (WO 02/47365 A2) in view of Ginter and in further view of Maillard et al. (US 2002/0048367 A1).

As per claim 3, Andreaux in view of Kaneko and further in view of Ginter discloses the method according to claim 1,

but fails to disclose expressly characterized in that a command is sent to the smart card for renewing the second key.

Maillard discloses characterized in that a command is sent to the smart card for renewing the second key. Maillard, page 4, paragraphs 58 and 59, describes a method including a command sent to the tamper resistant module for the renewing of the key

Andreaux and Maillard are analogous art because they are from the same field of endeavor of cryptography.

It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate the method of monitoring the usage of service as taught by Andreaux with the method of sending a command to the tamper resistant module for renewing the key as described by Maillard because it would prevent the data from being reproduced- Maillard, page 1, paragraph 9, lines 4 and 5.

As per claim 5, Andreaux in view of Kaneko and further in view of Ginter and Maillard discloses the method according to claim 3, characterized in that said command is encrypted by a third key known by the smart card. - Maillard, page 4, paragraphs 58 and 59, additional key stored on smart card.

As per claim 7, Andreaux in view of Kaneko and further in view of Ginter discloses the method according to claim 1,

but fails to disclose expressly "characterized in that, each first key is sent periodically, and in that the amount of data is converted into time of use limiting the use of a service in time.

However, Maillard discloses characterized in that, each first key is sent periodically, - Maillard, page 4, paragraph 58, lines 4 through 7, the encryption key changed monthly hence periodically

and in that the amount of data is converted into time of use limiting the use of a service in time. - Maillard, page 1, paragraph 11, the key is updated periodically according to the subscription. When user terminates subscription they would not retrieve the new key in order to continue decrypting data. Hence the service is limited to time of subscription.

Andreaux and Maillard are analogous art because they are from the same field of endeavor of cryptography.

It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate the method of sending a command to the tamper resistant module for renewing the encryption key periodically as described by Maillard with the method of monitoring the usage of service as taught by Andreaux because it would prevent the data from being reproduced -

Maillard, page 1, paragraph 9, lines 4 and 5 and it would allow for subscriptions to a data access service - Maillard, page 1, paragraph 11.

As per claim 12, Andreaux in view of Kaneko and further in view of Ginter and Maillard discloses the method according to claim 5, characterized in that said commands are transmitted to the smart card by way of the communication device, said communication device including a program for authorizing the transmission of such commands without reading its content – Andreaux, Figure 1, teaches the transmission of data.

6. Claims 4 and 8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Andreaux in view of Keneko and further in view of Ginter and Cutino et al. (EP 1263230 A1).

As per claim 4, Andreaux in view of Kaneko and further in view of Ginter discloses the method according to claim 1,

but fails to disclose expressly "characterized in that a command is sent to the smart card for Resetting/Updating the counter.

Cutino discloses characterized in that a command is sent to the tamper resistant module for Resetting/Updating the counter. - Cutino, column 9, lines 4 through 8, counter is decremented per use, value can be added to card hence updating the counter

Andreaux and Cutino are analogous art because they are from the same field of endeavor of cryptography.

It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate the method of updating the counter as described by Cutino with the smart card as

taught by Andreaux because it is desirable to store monetary value on a card and later replenish it - Cutino, column 9, lines 1 through 8.

As per claim 8, Andreaux in view of Kaneko and further in view of Ginter and cutino discloses the method according to claim 4, characterized in that said commands are transmitted to the smart card by way of the communication device, said communication device including a program for authorizing the transmission of such commands without reading its content – Andreaux, Figure 1, teaches the transmission of data.

7. Claim 11 is rejected under 35 U.S.C. 103(a) as being unpatentable over Andreaux in view of Kaneko and further in view of Ginter and Cutino and Maillard.

As per claim 11, Andreaux in view of Kaneko and further in view of Ginter and Cutino discloses the method according to claim 4.

But fails to disclose explicitly characterized in that said command is encrypted by a third key known by the smart card.

However, Maillard discloses characterized in that said command is encrypted by a third key known by the smart card - Maillard, page 4, paragraphs 58 and 59, additional key stored on smart card.

Andreaux and Maillard are analogous art because they are from the same field of endeavor of cryptography.

It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate the method of sending a command to the tamper resistant module for renewing the

key as described by Maillard with the method of monitoring the usage of service as taught by Andreaux because it would prevent the data from being reproduced- Maillard, page 1, paragraph 9, lines 4 and 5.

Conclusion

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Simon Kanaan whose telephone number is (571) 270-3906. The examiner can normally be reached on Monday to Friday 8:30 AM to 5:00 PM.

If attempts to reach the above noted Examiner by telephone are unsuccessful, the Examiner's supervisor, Gilberto Barron, can be reached at the following telephone number: (571) 272-3799.

The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system.

/SIMON KANAAN/
Examiner, Art Unit 2432

/Gilberto Barron Jr./
Supervisory Patent Examiner, Art Unit 2432